Test Procedure for §170.302 (u) General Encryption

This document describes the draft test procedure for evaluating conformance of complete EHRs or EHR modules[1] to the certification criteria defined in 45 CFR Part 170 Subpart C of the Final Rule for Health Information Technology: Initial Set of standards, Implementation Specifications, and Certification Criteria for Electronic Health Record Technology as published in the Federal Register on July 28, 2010. The document[2] is organized by test procedure and derived test requirements with traceability to the normative certification criteria as described in the Overview document located at http://healthcare.nist.gov/docs/TestProcedureOverview_v1.pdf. The test procedures may be updated to reflect on-going feedback received during the certification activities.

The HHS/Office of the National Coordinator for Health Information Technology (ONC) has defined the standards, implementation guides and certification criteria used in this test procedure. Applicability and interpretation of the standards, implementation guides and certification criteria to EHR technology is determined by ONC. Test procedures to evaluate conformance of EHR technology to ONC's requirements are defined by NIST. Testing of EHR technology is carried out by ONC-Authorized Testing and Certification Bodies (ATCBs), not NIST, as set forth in the final rule establishing the Temporary Certification Program (*Establishment of the Temporary Certification Program for Health Information Technology, 45 CFR Part 170; June 24, 2010*.)

Questions about the applicability of the standards, implementation guides or criteria should be directed to ONC at ONC.Certification@hhs.gov. Questions about the test procedures should be directed to NIST at hit-tst-fdbk@nist.gov. Note that NIST will automatically forward to ONC any questions regarding the applicability of the standards, implementation guides or criteria. Questions about functions and activities of the ATCBs should be directed to ONC at ONC.Certification@hhs.gov .

CERTIFICATION CRITERIA

This Certification Criterion is from the Health Information Technology: Initial Set of Standards, Implementation Specifications, and Certification Criteria for Electronic Health Record Technology Final Rule issued by the Department of Health and Human Services (HHS) on July 28, 2010.

§170.302(u) General encryption. Encrypt and decrypt electronic health information in accordance with the standard specified in §170.210(a)(1), unless the Secretary determines that the use of such algorithm would pose a significant security risk for Certified EHR Technology.

[1] Department of Health and Human Services, 45 CFR Part 170 Health Information Technology: Initial Set of Standards, Implementation Specifications, and Certification Criteria for Electronic Health Record Technology, Final Rule, July 28, 2010.

[2] Disclaimer: Certain commercial products are identified in this document. Such identification does not imply recommendation or endorsement by the National Institute of Standards and Technology.

Per Section III.D of the preamble of the Health Information Technology: Initial Set of Standards, Implementation Specifications, and Certification Criteria for Electronic Health Record Technology, Final Rule where the general encryption certification criterion is discussed:

- "Certified EHR Technology must include the capability to encrypt and decrypt information regardless of the transmission method used. This certification criterion and related standard do not specify the circumstances under which encryption and decryption must be performed; they simply require the capability."
- "If an eligible professional or eligible hospital determines that encryption is an appropriate and necessary safeguard, we believe that Certified EHR Technology should provide the capability to implement encryption. Overall, we want to ensure that Certified EHR Technology is capable of assisting eligible professionals and eligible hospitals to implement more secure technical solutions if they determine, based on their risk analysis, that technical safeguards such as encryption are reasonable and appropriate, or required."
- "We require that Certified EHR Technology must be capable of encrypting electronic health information. We do not specify the policies surrounding the use of encryption by an eligible professional or eligible hospital nor do we specify that it should only apply to devices. Rather we intend for Certified EHR Technology to be technologically capable of encryption, thereby allowing, if desired or required, an eligible professional or eligible hospital who adopts Certified EHR Technology to use this capability."

INFORMATIVE TEST DESCRIPTION

This section provides an informative description of how the test procedure is organized and conducted. It is not intended to provide normative statements of the certification requirements.

This test evaluates the capability for a Complete EHR or EHR Module to encrypt and decrypt electronic health information using an encryption algorithm specified in the standard.

The Vendor supplies the test data for this test procedure.

This test procedure is organized into two sections:

- Encrypt electronic health information – evaluates the capability to transform electronic health information into an unreadable format using an algorithm from the specified standard.
    - The Tester encrypts electronic health information according using a symmetric algorithm
    - The Tester validates that the electronic health information is unreadable

- Decrypt electronic health information – evaluates the capability to transform electronic health information into a readable format
    - The tester decrypts the electronic health information using a decryption function
    - The tester validates that the electronic health information is readable

REFERENCED STANDARDS

§170.210(a)(1)	Regulatory Referenced Standard
(a) Encryption and decryption of electronic health information (1) General. Any encryption algorithm identified by the National Institute of Standards and Technology (NIST) as an approved security function in Annex A of the Federal Information Processing Standards (FIPS) Publication 140-2 (incorporated by reference in §170.299).	§170.299 (i) National Institute of Standards and Technology, http://csrc.nist.gov/groups/STM/cmvp/standards.html (1) Annex A: Approved Security Functions for FIPS PUB 140-2, Security Requirements for Cryptographic Modules, Draft, January 27, 2010, IBR approved for §170.210.

NORMATIVE TEST PROCEDURES

Derived Test Requirements

DTR170.302.u – 1: Encrypt electronic health information

DTR170.302.u – 2: Decrypt electronic health information

DTR170.302.u – 1: Encrypt electronic health information

Required Vendor Information

VE170.302.u – 1.01: The vendor shall provide EHR documentation that specifies encryption and decryption capabilities and identifies algorithm and encryption key specifications used

VE170.302.u – 1.02: The vendor shall identify test data available for this test

Required Test Procedure:

TE170.302.u – 1.01: Examine Vendor-provided EHR documentation to determine if the vendor-identified encryption function utilizes an algorithm specified by the standard.

TE170.302.u – 1.02: Using the Vendor-provided test data, the tester shall encrypt the test data using the encryption function

TE170.302.u – 1.03: The tester shall verify that the encrypted test data is unreadable

Inspection Test Guide:

IN170.302.u – 1.01: Tester shall verify that Vendor encryption function utilizes an algorithm specified by the standard

IN170.302.u – 1.02: Tester shall verify that the encrypted electronic health information is unreadable

DTR170.302.u – 2: Decrypt electronic health information

Required Vendor Information

- As defined in DTR170.302.u – 1, no additional information is required

Required Test Procedure:

TE170.302.u – 2.01: The tester shall decrypt the encrypted test data using the decryption function

TE170.302.u – 2.02: The tester shall verify that the decrypted data is readable

Inspection Test Guide:

IN170.302.u – 2.01: Tester shall verify that the decrypted electronic health information is readable

TEST DATA

This Test Procedure requires the vendor to supply the test data. The Tester shall address the following:

- Vendor-supplied test data shall ensure that the functional and interoperable requirements identified in the criterion can be adequately evaluated for conformance
- Vendor-supplied test data shall strictly focus on meeting the basic capabilities required of an EHR relative to the certification criterion rather than exercising the full breadth/depth of capability that an installed EHR might be expected to support
- Tester shall record as part of the test documentation the specific Vendor-supplied test data that was utilized for testing

CONFORMANCE TEST TOOLS

None

Document History

Version Number	Description of Change	Date Published
0.2	Original draft version	April 8, 2010
1.0	Updated to reflect Final Rule	July 21, 2010
1.0	Updated to remove “Pending” from header	August 13, 2010